

Notice of Allowability	Application No.	Applicant(s)
	09/892,371	PEINADO, MARCUS
	Examiner	Art Unit
	Thomas M. Ho	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTO-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to 8/23/05.
2. The allowed claim(s) is/are 1-22.
3. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All
 - b) Some*
 - c) None
 of the:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) hereto or 2) to Paper No./Mail Date _____.
 - (b) including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. Notice of References Cited (PTO-892)
2. Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. Notice of Informal Patent Application (PTO-152)
6. Interview Summary (PTO-413),
Paper No./Mail Date _____.
7. Examiner's Amendment/Comment
8. Examiner's Statement of Reasons for Allowance
9. Other _____.

E. L. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

EXAMINER'S AMENDMENT

1. Claims 1-22 are pending.
2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Steven H. Meyer, Reg No. 37,189, at (215) 568-3100.

Independent claim 15 includes the recitation "the t second device" in the first statement of the claim. This has been amended to recite meant to recite "the second device".

Reasons for Allowance

3. In light of Applicant's amendments to claims 1 and 15, the previous rejections in view of Saito have been withdrawn.

In reference to claim 1:

A method for a user at a second computing device to render encrypted digital content on a first computing device distinct from the second device, the first device having a public key (PU1) and a corresponding private key (PR1), the second device having a public key (PU2) and a corresponding private key (PR2), the digital content being encrypted according to a content key (KD), the method comprising:

- *Where the user at the second computing device is the first user U1, and the computer or the client the first user U1 is requesting from is the second computing device.*
- *Where the first device's public key, PU1 is the public key presented to it by the first user, Kb1, and the corresponding private key to PR1 is Ks1.*
- *Where the second device public key PU2 is also Kb1 of the first user of Saito. Where the second device PR2 is Ks1 in Saito.*
- The user at the second device obtaining from a licensor distinct from the second device a digital license corresponding to the content and the second device, the digital license including the content key (KD) therein encrypted according to the public key (PU2) of the second device (PU2 (KD));
 - *Where the user at the second device is first user U1 in Saito, and where U1 obtains from the licensor(the data management center of Saito (Figure 1) distinct from U1)) the digital license (the combination of the data content name and Kb1 in Column 6, lines 60-67), where the content key*

KD is Ks1, and its encryption is present in Saito as Cks1kb1, where the public key PU2 used to encrypt KD is Kb1 of Saito.

- The user at the second device determining that the rules of the license do in fact permit issuance of a sub-license from the second device to the first device;
 - *Where the user at the second device is U1, and the issuance of a sub-license if performed by transferring the data content to a second user, U2. (Column 6, lines 43-47)*
- The user at the second device decrypting (PU (KD)) from the digital license with the corresponding private key (PR2) to produce the content key (KD);
 - *Where the content key KD, was encrypted as PU(KD) as Cks1kb1, and where the private key, PR2 is used to decrypt Cks1Kb1 to obtain the content key KD as Ks1 of Saito..*
- The user at the second device obtaining from the first device the public key thereof (PU1);
 - *Where the second device is U1 of Saito, and the public key PU1, as Kb1 of Saito is returned to the U1 in (Column 6, lines 60-67)*
- The user at the second device encrypting the content key (KD) according to the public key (PU1) of the first device (PU1 (KD)); and
 - *Where the user at the second device is U1 of Saito, and the content key, Ks1, is encrypted by the public key PU1(mapped to Kb1 of saito) to form Cks1kb1.*

Art Unit: 2134

Saito fails to disclose:

- The user at the second device composing the sublicense corresponding to and based on the obtained license for the first device, the sub-license including (PU1 (KD)), and transferring the composed sub-license to the first device, wherein the first device can decrypt (PU1 (KD)) with the private key thereof (PR1) to produce the content key (KD), and can render the encrypted content on the first device with the produced content key(KD).

Saito only discloses:

A sublicense containing PU1. (Column 6, lines 43-47)

Saito fails to disclose

- including rules for determining whether the license permits issuance of a sub-license from the second device to the first device;

Saito instead discloses the issuance of a sub-license (*Column 8, lines 37-48*) or (*Column 6, lines 43-47*), but fails to explicit state that rules are included to see if such action is permitted.

Additionally, the Examiner notes that the manipulations performed by Saito and Applicant's invention are very similar with the mappings shown above. The Examiner has mapped:

- PU1 as Kb1

- PR1 as Ks1
- PU2 as Kb1
- PR2 as Ks1
- KD as Ks1

However, in the art of cryptography however, Kb1 cannot be said to be equivalent to PU1 and PU2 and KD. The Applicant clearly has them as distinct entities in claim 1, while Kb1 in Saito assumes the role of all of them as a *singular* key. However, in the interest of the clarifying the reasons for allowance, the Examiner has mapped Kb1 to all of them to elucidate the similarity in the roles performed by Kb1 to the keys of Applicant's invention. Yet because Applicant has claimed three disparate keys, while Saito only uses one to perform these roles, it is the Examiner's position that Saito fails to disclose PU2 and KD.

For this reason, Claim 1 is distinguished from the prior art of record and the rejections are withdrawn. No art has been found to disclose nor motivation been found to further divide Kb1 into further disparate keys. Moreover, Saito actually further divides the secret key Ks1, and Ks1 into Ks11 and Ks12 in (Column 7, lines 35-45). A number of "key divisions" are further made in varying implementations throughout Saito, none of which divide the functionality of Kb1 into the roles that Applicant has distinguished in Claim 1.

Thus while, the division of a particular cryptographic role of a key into several keys is well known in the art as evidenced by Saito, there is no disclosure or motivation to divide the roles of the keys in the way that Claim 1 has recited.

For the reasons established above claim 1 is allowable.

Claim 15 is substantially similar to claim 1 and is allowable for the same reasons.

Claims 2-14, 16-22 depend upon independent claims 1 and 15 respectively. They are allowable in light of their independent claims being allowable.

Conclusion

4. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

Art Unit: 2134

General Information/Receptionist Telephone: 571-272-2100 Fax: 571-273-8300

Customer Service Representative Telephone: 571-272-2100 Fax: 571-273-8300

TMH

Feburary 5th, 2006